9110-18

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2020-0029]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security, United States Secret Service.

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "Department of Homeland Security/United States Secret Service-001 Criminal Investigation Information System of Records." This system of records describes the collection and maintenance of records by DHS/United States Secret Service (USSS) in its investigations related to individuals being investigated in connection with the criminal law enforcement functions of USSS, including investigating counterfeiting offenses, financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, and electronic funds transfer fraud. In this system of records notice update, DHS/USSS is modifying the categories of records, routine uses, and retention and disposal of records. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication. New or modified routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2020-0029 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Constantina Kozanas, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2020-0029. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: E. Gayle Rucker, (202) 406-5838, PrivacyServicesProgram@usssd.dhs.gov, Privacy Officer, United States Secret Service, Washington, D.C. 20223. For privacy questions, please contact: Constantina Kozanas, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, the Department of Homeland Security (DHS)/United States Secret Service (USSS) proposes to modify and reissue a current DHS system of records titled, "DHS/USSS-001 Criminal Investigation Information System of Records." The purpose of this system is to collect

and maintain criminal records related to individuals being investigated by DHS/USSS in connection with USSS' criminal law enforcement functions, including investigating counterfeiting offenses, financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, and electronic funds transfer fraud.

DHS/USSS is updating this system of records notice (SORN) to:

1) update the categories of records to consolidate the name category by grouping together variations of name types; (2) update the categories of records to consolidate the government-issued identifiers of persons by grouping together variations of government-issued identifiers of persons; (3) update the categories of records to consolidate the address category by grouping together variations of address types including other contact information identifiers; (4) update the categories of records to add citizenship and immigration information identifiers; (5) update the categories of records to add video imagery records; (6) update the categories of records to add historical cell-site location information; (7) update the categories of records to add geo-fence records of mobile devices; (8) update the categories of records to add government-issued identifiers of property; (9) update the categories of records to add biometric identifiers and profiles based on biometric attributes; (10) update the categories of records to add samples of deoxyribonucleic acid (DNA) and their DNA profiles; (11) update the categories of records to add social media posts, profiles, and account content; (12) modify routine use (E) and add new routine use (F) to conform to Office of Management and Budget Memorandum M-17-12; (13) modify previously issued routine use (I), now routine use (N), to remove disclosures "in response to a subpoena"; (14) add routine use (P) for disclosure to government agencies for the purposes of testing new technology; (15)

remove routine uses that are no longer applicable; and (16) update retention and disposal of records to reflect the most recent National Archives and Records Administration (NARA)-approved records schedules.

Further, DHS is making non-substantive changes to the text and formatting of this SORN to align with previously published DHS SORNs, to include the reordering and re-lettering of routine uses.

Consistent with DHS's information sharing mission, information stored in the DHS/USSS-001 Criminal Investigation Information System of Records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/USSS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and

amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/USSS-001 Criminal Investigation Information System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: Department of Homeland Security (DHS)/United States Secret Service (USSS)-001 Criminal Investigation Information System of Records.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Records are maintained at the USSS Headquarters in Washington, D.C. and field offices. IT systems covered by this SORN include USSS systems, such as e-Agent, Field Support System (FSS), and Field Investigative Reporting System (FIRS), all accessible at USSS offices.

SYSTEM MANAGER(S): Assistant Director, Office of Investigations, United States Secret Service, wfo@usss.dhs.gov, 245 Murray Lane SW, Building T-5, Washington, D.C. 20223.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The Homeland Security Act of 2002, Public Law 107-296, including 6 U.S.C. sec. 124n, 6 U.S.C. sec. 455, and 6 U.S.C. sec. 383; 18 U.S.C. sec. 3056; 18 U.S.C. sec. 3056A; 18 U.S.C. sec. 1029(d); 18 U.S.C. sec. 1030(d).

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to collect and maintain criminal records related to individuals being investigated by DHS/USSS in connection with DHS/USSS' criminal law enforcement functions, including investigating

counterfeiting offenses, financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, and electronic funds transfer fraud.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals in this system of records include: (1) individuals who have been or are currently the subject of a criminal investigation by DHS/USSS in connection with the performance by that agency of its authorized criminal investigative functions; (2) individuals who are informants, suspects, defendants, fugitives, released prisoners, victims, witnesses, or those associated with these individuals who have been identified by DHS/USSS during the course of official DHS/USSS criminal investigations or by information supplied by other law enforcement agencies, units, and the general public; (3) individuals who are complainants and correspondents; (4) individuals who are payees, registered owners, or endorsers of stolen or lost obligations and other securities of the United States; and (5) USSS and other law enforcement personnel.

CATEGORIES OF RECORDS IN THE SYSTEM:

- Name, alias, or code name;
- Records containing information from government-issued identifiers, including Passport number, Social Security number, and Driver License number;
- Contact information identifiers, such as physical and electronic addresses and phone numbers;
- Records containing still and video imagery (imagery records containing facial biometrics may be both electronically analyzed and/or examined by human agents during the course of criminal investigations);

- Records containing historical cell-site location information obtained from providers of electronic communications, and other information lawfully obtained under the provisions of 18 U.S.C. sec. 2701, et seq.;
- Records containing citizenship information and identifiers;
- Records containing geo-fence information from mobile devices to track a suspected criminal's location;
- Records containing information from government-issued property identifiers, to include boat, vehicle, and other asset registration numbers;
- Social media posts, profiles, and account content;
- Records containing information from biometric identifiers and profiles based on biometric attributes to include fingerprint and voiceprint (such information may be both electronically analyzed and/or examined by human agents); and
- Records containing information from DNA samples and profiles of DNA obtained from the body, such as bodily fluids, or obtained from contacted surfaces (such information may be both electronically analyzed and/or examined by human agents).

RECORD SOURCE CATEGORIES: The Secretary of Homeland Security has exempted this system from subsections (e)(4)(I) of the Privacy Act pursuant to 5 U.S.C. secs. 552a(j)(2), (k)(2), and (k)(3); therefore, record source categories shall not be disclosed.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a

portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorney's Offices, or other federal agencies conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To NARA or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the federal

government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another federal agency or federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the federal government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To employees and officials of financial and commercial business firms and to private individuals, information pertaining to actual or suspected criminal offenders

where such disclosure is considered reasonably necessary for the purpose of furthering USSS efforts to investigate the activities of and apprehend criminal offenders and suspected criminal offenders.

J. To federal, state, and local government agencies foreign or domestic, having prosecutorial and civil law enforcement functions for use by attorneys, magistrates, and judges, parole or probation authorities and other law enforcement authorities for the purpose of developing a criminal or civil investigation, prosecuting, sentencing, or determining the parole and probation status of criminal offenders or suspected criminal offenders.

K. To personnel of other federal, state, and local law enforcement agencies, foreign or domestic, for the purpose of developing information on subjects involved in USSS criminal investigations and assisting other law enforcement agencies in the investigation and prosecution of violations of the criminal laws which those agencies are responsible for enforcing.

L. To personnel of federal, state, and local governmental agencies, foreign and domestic, where such disclosure is considered reasonably necessary for the purpose of furthering USSS efforts to investigate the activities of and apprehend criminal offenders and suspected criminal offenders.

M. To personnel of federal, state, and local governmental agencies, foreign and domestic, where there is a showing of reasonable necessity to obtain such information to accomplish a valid law enforcement purpose as agreed to by the USSS.

N. To a court, magistrate, or administrative tribunal in the course of presenting evidence and opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal or civil proceedings.

O. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or the issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, the issuance of a license, grant, or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

P. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data for purposes of testing new technology that relate to the purpose(s) stated in this SORN.

Q. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/USSS stores records in this system electronically or on paper in secure facilities behind a locked door. The electronic records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS/USSS may retrieve records by name, address, vehicle license number, or other identifier retrieved

through computer search of electronic files maintained both at USSS Headquarters and in the field offices. Access to the physical files containing records is by case number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Investigative Records are managed by DHS/USSS in accordance with the following National Archives and Records Administration (NARA) approved records schedules: N1-087-89-02, "Field Investigative Records," N1-087-92-002, "Investigative Program Records," and NC1-87-84-1, "Closed Case Investigative Files." Records are retained, transferred, and destroyed based on where the record was created (Headquarters or Field Office) and the type of record. For instance, pursuant to N1-087-89-02, for Field Office records, all selected closed case files pursuant to the selection criteria in the introduction of N1-087-89-02 are permanent and are subsequently transferred to NARA 30 years after the case has ended. All other closed case files are retained, transferred, and destroyed in the following: criminal judicial case files are to be transferred to a Federal Records Center (FRC) and destroyed 30 years after the end of the case; criminal non-judicial case files are to be transferred to the FRC and destroyed 30 years after the end of the case, except for forgery case files which are to be transferred to the FRC and then destroyed 5 years after the end of the case; non-criminal case files are to be transferred to the FRC and then destroyed 5 years following the end of the case; and investigations for other district (IOD) cases are to be destroyed two years following the end of a case. Case files in Field Offices containing special information are to be retained for the following dependent on the type of information: Title I Intercept Material Electronic communications (minimum of 10 years), Protected IRS information (minimum of 8 years), and mail cover information (minimum of 8 years), and then all follow records retention schedule for closed investigative case files in Item 1 of N1-087-89-02. Please

refer to N1-087-89-02 for records retention schedules for other Field Office Investigative Program Records. Headquarters Office records are subject to NC1-87-84-1, as amended by N1-087-92-002. For instance, all selected closed case files pursuant to the selection criteria in the introduction of NC1-87-84-1 are permanent and are subsequently transferred to NARA in five-year blocks when 50 years old. Judicial, non-judicial, and non-criminal case files are to be transferred to the FRC 10 years after closing the case and destroyed 30 years after the end of the case. Please refer to NC1-87-84-1 and N1-087-92-002 for all other investigative program records held at USSS Headquarters. Disposal of records that have met the end of their life cycles is carried out in a secure manner, including by burning or shredding.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/USSS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/USSS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/USSS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Chief Freedom of

Information Act (FOIA) Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contact Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA Officer, Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief FOIA Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: This system of records is exempt from the Privacy Act's access and amendment provisions and those of the Judicial Redress Act; therefore, record access and amendment may not be available. In such cases, certain records about an individual may be available under FOIA, and the correspondence from those seeking a record amendment may be placed in the respective case file. For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. sec. 552a(c)(3) and (4); (d); (e)(1),

(e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), and (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(k)(1), (k)(2), and (k)(3) has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. sec. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I); and (f).

HISTORY: 76 FR 49497 (August 10, 2011); 74 FR 45087 (Final Rule) (August 31, 2009).

Constantina Kozanas,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2020-22533 Filed: 10/9/2020 8:45 am; Publication Date: 10/13/2020]